REMARKS

This is a full and timely response to the non-final Official Action mailed **June 5, 2008** (the "Office Action" or "Action"). Reconsideration of the application in light of the following remarks is respectfully requested.

Claim Status:

Claims 20-32 were cancelled in a previous paper. No amendments to the claims are proposed by the present paper. Thus, claims 1-19 are currently pending for further action.

Prior Art:

Claims 1-19 were rejected under 35 U.S.C. § 103(a) as obvious in light of the combined teachings of U.S. Patent No. 5,870,474 to Wasilewski et al. ("Wasilewski") and U.S. Patent No. 6,324,646 to Chen et al. ("Chen"). For at least the following reasons, this rejection is respectfully traversed.

Claim 1 recites:

> A method of providing varying levels of security in a data processing system, the method comprising:
> receiving information from an outside source;
> *retrieving a first indicator from the received information that instructs the system to operate at a higher level of security*;
> receiving further information from said outside source;
> retrieving a separate second indicator from said further information received from said outside source, *the second indicator for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator*;
> *receiving an encrypted message that authorizes the system to operate at the lower level of security*;

authenticating the encrypted message; and

preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator and the encrypted message; while

continuing operation of said processing system at the higher level of security.

(Emphasis added).

In contrast, Wasilewski does not teach or suggest the subject matter of claim 1. Rather, Wasilewski teaches a control system for conditional access to a media program in which "program bearing packets are encrypted according to a first encryption algorithm using a first key, which is then encrypted according to a second encryption algorithm using a second key. The first keys are transported in packets to the customer's set top units along with the program packets. A public key cryptographic technique encrypts the second key such that the public key used in the encryption corresponds to the private key of the customer's set top unit. After the conditional access layers have been added, the packets are encapsulated and output in a second network protocol destined for the set top unit." (Wasilewski, abstract).

In particular, Wasilewski completely fails to teach or suggest a system configured to operate at a higher (or lower) level of security in response to receiving an "indicator…that instructs the system to operate at a higher [or lower] level of security." (claim 1). Rather, Wasilewski merely teaches a system in which media content experiences multiple levels of encryption with different corresponding encryption keys prior to delivery to a set top box. (*See e.g.* Wasilewski, abstract and col. 11, lines 10-23). To maintain security, Wasilewski teaches that "frequent key changing is designed to thwart attempts by unauthorized users to compromise the encryption algorithm by discovering the key." (Wasilewski, col. 8, lines 48-52).

The recent Office Action improperly extrapolates from these teachings that Wasilewski's system is necessarily operating at a different level of security whenever an encryption/decryption

key is changed, thereby allegedly rendering obvious much of the subject matter of claim 1. (Action, pp. 3-4). However, this assertion is completely without basis and incongruous with the principles taught by Wasilewski. It will be readily apparent to anyone having ordinary skill in the art that the level of security at which data is transmitted and received is determined by the algorithm(s) used to encrypt the data, and not by the specific parameters (i.e. encryption keys) used by the algorithms to obtain unique encryption results. In other words, changing an encryption key in an encrypted system from a first value to a second value does not make the encrypted data any more or less inherently secure in its encryption. Instead, the security of the encryption is determined by the encryption algorithm itself, not by the parameters passed to the algorithm. Thus, without a change in the encryption algorithm itself, no measurable change in the security level of an encrypted system is feasible. Wasilewski does not teach or suggest any such change in any of the nested algorithms used to encrypt media content data. Thus, even though Wasilewski teaches that the keys used to encrypt data may be changed, Wasilewski does not teach or suggest a change in the actual level of security in data transmission. Wasilewski merely teaches *static* encryption algorithms with *dynamic* parameters.

Without teaching a change in the level of security, Wasilewski *cannot* teach much of the subject matter of claim 1. Specifically, Wasilewski *cannot* teach the steps of "receiving a first indicator from the received information that instructs the system to operate at a higher level of security," "retrieving a separate second indicator…for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator," receiving and authenticating "an encrypted message that authorizes the system to operate at the lower level of

security," and "preventing an operation at the lower level of security until a decrease in security levels is indicated by said second indicator and the encrypted message." (claim 1).

Turning now to Chen, it becomes readily apparent that Chen also does not teach or suggest much of the subject matter of claim 1. Chen teaches a data transmission protocol having a "security descriptor field identifier, whose implementation can be understood by communicating parties." (Chen, col. 6, lines 28-31). However, Chen does not teach or suggest that the security descriptor field identifier may be *dynamically changed by the communicating parties during the transmission of data* to alter the level of security in response to retrieving an "indicator from the received information that instructs the system to operate at a higher [or lower] level of security." (claim 1). Rather, Chen appears to merely teach that the data protocol used between communicating parties provides for flexibility in upgrading algorithms used to secure data transmitted between those parties.

Moreover, Chen does not teach or suggest anywhere that both an "indicator for instructing the system to operate at a lower level of security than the higher level of security" and "an encrypted message that authorizes the system to operate at a lower level of security" must be received in addition to the encrypted message being authenticated prior to a system switching from a higher level of security to a lower level of security. (claim 1). Chen simply does not teach or suggest this change in the level of security or the requirements that must be met to effect it.

Under the analysis required by *Graham v. John Deere*, 383 U.S. 1 (1966) to support a rejection under § 103, the scope and content of the prior art must first be determined, followed by an assessment of the differences between the prior art and the claim at issue in view of the

ordinary skill in the art. In the present case, the scope and content of the prior art, as evidenced by Wasilewski and Chen, did not include the claimed subject matter, particularly the following steps:

- "retrieving a first indicator from the received information that instructs the system to operate at a higher level of security;"
- "retrieving a separate second indicator from said further information…for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator;"
- "receiving an encrypted message that authorizes the system to operate at the lower level of security;"
- "authenticating the encrypted message;" and
- "preventing operation at the lower level of security until a decrease in security levels is indicated by said indicator and the encrypted message; while continuing operation of said processing system at the higher level of security."

(claim 1).

The differences between the cited prior art and the claimed subject matter are significant because the claimed method provides a way to "make a change from a low level of encryption to a high level of encryption in a relatively easy manner" without "[compromising a system] when a change is made from a high level of security to a low level of security." (Applicant's specification, p. 2, lines 4-7). Thus, the claimed subject matter provides features and advantages not known or available in the cited prior art. Consequently, the cited prior art will not support a rejection of claim 1 under 35 U.S.C. § 103 and *Graham*. For at least these reasons, the rejection of claim 1 and its corresponding dependent claims based on Wasilewski and Chen should be reconsidered and withdrawn.

Additionally, various dependent claims of the application recite subject matter that is further patentable over the cited prior art. Specific, non-exclusive examples follow.

Claim 2 recites "wherein the encrypted message comprises a Decreased-Security-Authorization-Code." Claims 3-5 impose additional limitations on the Decreased-Security-Authorization-Code. As has been amply demonstrated above, neither of Wasilewski and Chen teaches or suggests even the existence of an "encrypted message that authorizes the system to operate a lower level of security," let alone the additional limitations imposed on the encrypted message by dependent claims 2-5. The recent Office Action again attempts to assert that a change in an encryption key indicates a change in a level of security, an assertion that, as has been amply demonstrated above, is plainly incorrect. (Action, p. 5). For at least these additional reasons, the rejection of claims 2-5 should be reconsidered and withdrawn.

Claim 8 recites "establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented by the system." Claims 9-12 impose additional limitations on the claimed "Security-Level-Status-Indicator." In response, the recent Office Action cites to Wasilewski, col. 11 lines 10-50. (Action, p. 5). Nowhere in the cited reference or anywhere else in Wasilewski or Chen is this subject matter taught or suggested. Thus, these rejections are utterly improper. For at least these additional reasons, the rejection of claims 8-12 should be reconsidered and withdrawn.

Claim 14 recites "using a Key Management Message to convey said Decreased Security Authorization Code." Claims 15-17 recite further limitations on the Key Management Message. Again, with respect to these claims, the recent Office Action cites to the same portion of Wasilewski used elsewhere. (Action, p. 6; *See also* Wasilewski, col. 11 lines 10-50). Aside

from the utter irrelevance of the cited portion, as neither of Wasilewski and Chen teaches or suggests a Decreased Security Authorization Code at all, Wasilewski and Chen combined *cannot* teach or suggest "using a Key Management Message to convey said Decreased Security Authorization Code." For at least this additional reason, the rejection of claims 14-17 should be reconsidered and withdrawn.

Conclusion:

In view of the foregoing arguments, all claims are believed to be in condition for allowance over the prior art of record. Therefore, this response is believed to be a complete response to the Office Action. However, Applicant reserves the right to set forth further arguments in future papers supporting the patentability of any of the claims, including the separate patentability of the dependent claims not explicitly addressed herein. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed.

The absence of a reply to a specific rejection, issue or comment in the Office Action does not signify agreement with or concession of that rejection, issue or comment. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment. Further, for any instances in which the Examiner took Official Notice in the Office Action, Applicants expressly do not acquiesce to the taking of Official Notice, and respectfully request that the Examiner

provide an affidavit to support the Official Notice taken in the next Office Action, as required by 37 CFR 1.104(d)(2) and MPEP § 2144.03.

If the Examiner has any comments or suggestions which could place this application in better form, the Examiner is requested to telephone the undersigned attorney at the number listed below.

Respectfully submitted,

DATE: September 5, 2008

Steven L. Nichols
Registration No. 40,326

Steven L. Nichols, Esq.
Managing Partner, Utah Office
Rader Fishman & Grauer PLLC
River Park Corporate Center One
10653 S. River Front Parkway, Suite 150
South Jordan, Utah 84095

(801) 572-8066
(801) 572-7666 (fax)